Claims

1. Method for printing of sensitive data, comprising the following steps:
   - encryption at a workstation (2) of sensitive data to be printed,
   - transfer to a printing device (1) of the data to be printed,
   - decryption of the sensitive data to be printed,
   - conversion of the data to be printed into control signals for activation of a printing unit (9, 10, 11),
   - printing of the data on a recording medium,

   whereby the decrypted data are not stored in a readable format on a non-volatile storage medium between the decryption and the printing of the data.

2. Method according to claim 1,
characterized in that
the decrypted data are stored in a volatile memory such as, for example, RAM between the decryption and the printing.

3. Method according to claim 1,
characterized in that
the decrypted data are stored in a non-volatile memory between the decryption and the printing, whereby the data are distributed on a plurality of memory segments and their association is stored independent of the data, advantageously in RAM.

4. Method according to any of the claims 1 through 3,
characterized in that
the control signals containing sensitive data are stored in a volatile memory such as, for example, RAM.

5. Method according to any of the claims 1 through 3,

characterized in that
the control signals containing sensitive data are stored in a non-volatile memory, whereby the data are distributed on a plurality of memory segments and their association is stored independent of the data, advantageously in a volatile memory.

6. Method according to any of the claims 1 through 5, characterized in that
the decryption and the conversion into control signals is [sic] executed in immediate temporal succession.

7. Method according to any of the claims 1 through 5, characterized in that
the decryption and the conversion into control signals is executed in a controller (12) for activation of a character generator (10).

8. Method according to any of the claims 1 through 7, characterized in that
the data to be printed are transferred to the printing device in the form of a print data stream such as, for example, IPDS, PDF, PCL or PS,
the print data stream is converted into an intermediate language in the printing device, and
the print data are decrypted and converted into control signals.

9. Method according to any of the claims 1 through 8, characterized in that
the print data contain both sensitive data and non-sensitive data.

10. Method according to claim 9, characterized in that

the sensitive data and the non-sensitive data are connected into one data unit (such as, for example, a print file) before the transfer to the printing device.

11. Method according to claim 10,
characterized in that
the sensitive data are identified in the data unit via markings.

12. Method according to claim 10 or 11,
characterized in that
a layout that comprises regions to receive sensitive data is generated using the non-sensitive data.

13. Method according to any of the claims 10 through 11 [sic],
characterized in that
the sensitive data are already encrypted before the combination with the non-sensitive data into one data unit.

14. Method according to any of the claims 10 through 11,
characterized in that
the sensitive data are encrypted after the combination with the non-sensitive data into one data unit.

15. Method according to claim 14,
characterized in that
only the sensitive data are encrypted.

16. Method according to claim 14,
characterized in that
both the sensitive data and the non-sensitive data are encrypted.

17. Method according to any of the claims 1 through 16,
characterized in that
the conversion of the data to be printed into control signals for activation of a printing unit via rastering of the data to be printed into one or more raster images is excuted [sic], whereby the raster images represent the control signals.

18. Device for printing of sensitive data according to the method according to any of the claims 1 through 17, with
- a printing unit (9, 10, 11)
- a controller (12) for activation of the printing unit,
whereby the controller (12) is fashioned to receive a print data stream that can contain encrypted data, and that [sic] the sensitive data are decrypted and converted into control signals for activation of the printing unit,
whereby the decrypted data are not stored in a readable format on a non-volatile storage medium.

19. Device according to claim 18,
characterized in that
the printing unit comprises a character generator (10).

20. Device according to claim 18 or 19,
characterized in that
the device is an electrophotographic high-capacity printer.

21. Device according to any of the claims 18 through 20,
characterized in that
the controller (12) comprises a decryption module (16) and one or more raster modules (17).

22. Device according to any of the claims 18 through 20,

characterized in that
the controller (12) comprises a combined decryption/raster module.

23. Device according to any of the claims 18 through 22,
characterized in that
the controller (12) comprises only volatile storage media.

24. Device according to any of the claims 18 through 23,
characterized in that
a sensor for detection of recording media with predetermined security features is arranged on a transport path (6) for recording media in the region before the printing unit (9, 10, 11), such that the printing of sensitive data can be stopped given the detection of recording media without security features.